NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

Why You Can Trust CNET

Advertiser disclosure

Our expert, award-winning staff selects the products we cover and rigorously researches and tests our top picks. If you buy through our links, we may get a commission. Reviews ethics statement

Money

What Should You Do When You Receive a Data Breach Notice?

Don't treat your data breach letter like junk mail. Do this instead.

Geoff Williams

Dec. 24, 2024 4:35 a.m. PT

3 min. read



(Image credit: Getty Images)

Data breach notices tell us that our personal data was compromised. In 2024 alone, major data breaches occurred at National Public Data, Change Healthcare and Ticketmaster, putting millions of consumers at risk of financial fraud and identity theft.

"On average, we have seen eight to nine data breach incidents every day," said Weiqing Sun, director of master's programs in cybersecurity at the University of Toledo. "More frequent and more significant data breaches will occur and keep affecting every one of us."

TAX SOFTWARE DEALS OF THE WEEK

H&R Block Free Simple Tax Returns eFile: **$0** *(save $0)*

TurboTax Deluxe 2024 (Federal and State, PC/Mac Download):
$56 *(save $24)*

TurboTax Premier 2024 (Federal and State, PC/Mac Download):
$83 *(save $32)*

TaxSlayer Classic Plan: **$28** *(save $10)*

Deals are selected by the CNET Group commerce team, and may be unrelated to this article.

If you receive a data breach letter in the mail, don't ignore it. It will inform you that an unauthorized party has gained access to internal company data and may possess your personally identifiable information like your name, phone number, Social Security number and more.

Here's everything you should know about data breach notices.

What's in a data breach notice?

Data breach notices usually include the following information:

- Details about how and when the breach occurred
- A list of your personal data that might have been leaked to hackers
- An explanation of what the company is doing to protect your data in the aftermath
- Tips to help you keep your identity safe

Companies will regularly pay for free identity theft or credit monitoring services for affected customers. Activation codes are provided in the letter, but you must create the account yourself to take advantage of the offer. Depending on the severity of the breach, the free coverage lasts up to two years in most cases.

Identity theft protection services help monitor your sensitive data on the dark web. Sometimes, these services can alert you that your data has been compromised before you even receive a notice. Most importantly, they come with identity restoration services if your identity is stolen.

"Try to take advantage of those services to get the protection," said Sun.

When and how will a company send me a data breach notice?

All states, the District of Columbia, Puerto Rico, and the US Virgin Islands have passed laws requiring companies to notify customers of data breaches. The length of time varies by state, but notices are usually sent within 60 days after the data leak is discovered.

Advertisement

NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

Data breach notices come in the mail. If you receive a notice by email, text or phone call, it's likely a scam. If you have any doubts about the legitimacy of a notice claiming your sensitive data has been compromised, contact the company directly or search online for coverage of the breach, Sun said.

In addition to impacted customers, companies that suffer a cyberattack may alert state attorney general's offices, law enforcement, the three major credit bureaus, and the Securities and Exchange Commission, depending on the severity of the breach or state regulations.

What should I do if I receive a letter in the mail?

If you receive notice of a data breach by mail, follow the advice in the letter and take it seriously. You should be on the lookout for phishing attacks and regularly check your Experian, TransUnion and Equifax credit reports for unauthorized accounts opened in your name.

If the company offers free identity theft protection, sign up for it. After the membership expires, you'll need to decide whether to pay to continue with the service or subscribe to another provider.

Aura

CNET's pick for the best identity theft protection service

See at Aura

Protect your personal data and get peace of mind with CNET's top pick for identity theft protection.

Advertisement

NAVIGATING A WORLD OF ACCELERATING CHANGE CNET

If your data is involved in another data breach in the future, you may sign up for additional free services offered to you later.

What are some steps I can take to protect my data?

Even if you aren't using an ID theft protection service, here are four things you can do for free to protect yourself:

1. Change your password on the breached account, along with any other accounts with the same login credentials.

2. Review your credit card and debit card statements at least once a month and look for any abnormalities

3. Freeze your credit so that nobody can apply for a line of credit in your name (you'll have to unfreeze it yourself if you want to open a new account)

4. Remain vigilant of phishing attacks by cybercriminals using your leaked information to trick you into sharing financial account information or other sensitive data

The editorial content on this page is based solely on objective, independent assessments by our writers and is not influenced by advertising or partnerships. It has not been provided or commissioned by any third party. However, we may receive compensation when you click on links to products or services offered by our partners.

© 2025 CNET, a Ziff Davis company. All rights reserved.